symantec™

Norton™ Personal Firewall 3.0

For Macintosh®

User's Guide

Norton™ Personal Firewall for Macintosh® User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 2003 Symantec Corporation. All Rights Reserved.

Documentation version 3.0

PN: 10067433

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Norton and LiveUpdate are trademarks of Symantec Corporation.

Macintosh, MacOS, Macintosh PowerPC, Macintosh G3, and Finder are trademarks of Apple Computer, Inc. Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Symantec License and Warranty

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. License:

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;

C. use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network; and

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

F. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty (60) day period following the delivery to you of the Software.

4. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements

or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

5. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

6. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

Contents

Chapter 1 About Norton Personal Firewall for Macintosh

What's new in Norton Personal Firewall 9
What can happen without a firewall 10
How Norton Personal Firewall works 10
    How to determine which computers get access 11
Is my computer protected now? 11

Chapter 2 Installing Norton Personal Firewall

System requirements 13
Before installation 13
    Read the Read Me file 14
Installation 14
After installation 18
    Restart your computer 18
    Register Norton Personal Firewall 19
    Read Late Breaking News 20
    If you connect to the Internet through America Online 20
If you need to uninstall Norton Personal Firewall 21

Chapter 3 Norton Personal Firewall basics

How to open and exit Norton Personal Firewall 23
Check your firewall settings 24
Disable and enable firewall protection 26
    Disable Norton Personal Firewall temporarily 27
Customize your toolbars 27

For more information 28
Access Help 28
Access the User's Guide PDF 29
Open the Read Me file 29
Explore the Symantec support Web site 30

Chapter 4 Protecting disks, files, and data from intrusion
What Norton Personal Firewall protects 31
Specify access by IP address or host name 32
Define protection for port numbers 32
Track access attempts 33
Norton Personal Firewall and AppleTalk 33
TCP/IP security on Norton Personal Firewall 33

Chapter 5 Monitoring access attempts
Monitor firewall activity 35
Enable or disable notification of access attempts 36
Test firewall settings 37
Respond to access attempts 40
About alert messages 40
View the Access History log 41
Learn more about a specific access attempt 43
Change logging preferences 45
Disable logging 45
How the log file is structured 46
Work with the Connected Users report 47
Change the appearance of the Connected Users report 48
Disconnect a connected user 49
Get more information about a connected user 49
Export the Connected Users list 50
Change the time limit for disconnected users 50

Chapter 6 Customizing firewall protection
Set protection for standard Internet services 51
Add IP addresses 52
Add subnet addresses 53
Define a custom service to protect 54
Edit or delete a custom service 55
Change protection settings 55
Change the level of restriction 55
Change an IP address list 56
About active FTP support 57

Stealth mode 57
What Stealth mode does 57
Disable Stealth mode 57
Block suspicious activity 58
About UDP 58
Enable UDP protection 59
How UDP protection works 59

Chapter 7 Troubleshooting in Norton Personal Firewall
Frequently asked questions 61
How do I turn off firewall protection? 61
Why can't I access any Web site? 61
What service does this port number represent? 62
How do I create a new log file? 65
Why doesn't Norton Personal Firewall load? 66
Why doesn't File Sharing work? 66
Why can't I install Norton Personal Firewall for Mac OS X? 66
Why can't I create an alias to Norton Personal Firewall? 66
My entries in IPFW keep disappearing 66
Questions about home networking 67
How do I protect all of the computers on my home network? 67
How do I specify access for a computer with a dynamically generated IP address? 67
How does the firewall affect file and printer sharing? 67

Chapter 8 Keeping Norton Personal Firewall up-to-date
About program updates 69
When you should update 70
Before updating 70
If you use America Online to connect 70
If you update on an internal network 70
If you can't use LiveUpdate 71
Update procedures 72
Update everything now 72
Customize a LiveUpdate session 72
After updating 73
View the LiveUpdate Summary 73
Empty the Trash after a LiveUpdate session 73
Check product version numbers and dates 73
Schedule future updates 74

Chapter 9 Scheduling future events
About Norton Scheduler 75
Open Norton Scheduler 75
Schedule LiveUpdate events 76
Set a start time 77
Manage scheduled events 77
Edit scheduled events 77
Delete scheduled events 77
Disable scheduled events 78
Reset scheduled tasks 78

Service and support solutions

Glossary

Index

CD Replacement Form

About Norton Personal Firewall for Macintosh

1

When you connect to the Internet (the global network of computers), you can connect with millions of other computers. Those computers can also connect with your computer. Unprotected connections to the Internet leave your computer vulnerable to hacker attacks, viruses, *Trojan horses*, and many other Internet *threats*. (Hackers are people who break into computers without permission. Viruses and Trojan horses are programs that can corrupt the data on your computer.)

Norton Personal Firewall for Macintosh helps you monitor and control connections to your computer. It helps protect your security and privacy.

What's new in Norton Personal Firewall

Version 3.0 of Norton Personal Firewall for Macintosh now includes:

- Setup Assistant, which walks you through your computer's Internet service settings and provides an easy way to set up the firewall to work with those settings.
- Automatic setup of your firewall for any active *services*. After installing Norton Personal Firewall, if you start a service on your computer, automatic setup checks your firewall settings and warns you if any of them will interfere with your use of that service.
- The Connected Users report, which shows you all other computers that are currently connected to your computer.
- Logging and notification options, which can be specified individually for each service on your computer.

- Outgoing connection firewall settings to help you control the use of your computer and thwart malicious programs that may send data without your knowledge.
- The Norton QuickMenu, which appears in the menu bar at the top of the screen and provides you with access for opening, disabling, and enabling Norton Personal Firewall.
- Improved protection options, such as suspicious activity protection to block transmission of data with forged *IP addresses*, an option to allow access for essential services when *UDP* protection is on, and an option to turn off active *FTP* support.
- The ability to specify an IP address other than your own computer's during Self Test.

What can happen without a firewall

When you are connected to the Internet or another network, others connected to that network can access your computer. This situation can be dangerous if you have enabled File Sharing or program linking, making your computer vulnerable to hackers.

How Norton Personal Firewall works

Norton Personal Firewall provides a firewall between your computer and the Internet. Firewall programs are filters that block or allow connections over the Internet. By filtering connections, firewalls protect your computer from malicious Internet activity.

Norton Personal Firewall uses access settings to determine whether to permit or block connections. You can change these settings, permitting or blocking other computers from accessing your computer, and permitting or blocking connections from your computer.

You specify the *services* that you want to protect (such as Web Sharing or File Sharing) and from which computers. You can allow or deny all access to a particular service, or allow or deny access to a service from certain computers. For example, you can block all access to File Sharing while allowing access to Web Sharing for computers belonging to people who you know.

You can also block outgoing connections from your computer. You can do this to control usage of your computer. For example, if you have two

computers that are networked and you want only one of them to have Internet access, you can block outgoing Web Sharing access on the other computer. You can also block outgoing connections to prevent *Trojan horses* and other malicious programs from sending data from your computer without your knowledge.

How to determine which computers get access

In most cases, you do not need to allow anyone access to your computer. However, following are some computer configurations and Web and file sharing situations that require you to allow access:

- You have two or more computers networked, and at least one has Internet access. In this case, every computer with Internet access needs a copy of Norton Personal Firewall installed, with access allowed only to the other computers on the network.
- You have a Web site on your computer to which you want to restrict access. Using Norton Personal Firewall, specify Web Sharing access to those whom you want to see your site such as other family members.
- You are using a free Internet service provider that may require access to a *port* on your computer to maintain your connection. If the *ISP* is not granted that access, you lose the service.

See "Respond to access attempts" on page 40.

When installed, Norton Personal Firewall is set to log all incoming access attempts, except those that are related to Stealth mode. You can always check the Access History window to see if someone isn't getting through who should.

Is my computer protected now?

Once you have installed Norton Personal Firewall and restarted your computer, the firewall is in place, set by default to block all incoming access attempts. As you work with Norton Personal Firewall, you can adjust your access settings as necessary.

With Norton Personal Firewall installed, you can continue to use your computer as you always have and you will notice no difference. This is exactly how it's supposed to work. The firewall is in place, stopping any unwanted intrusions.

Installing Norton Personal Firewall

2

Before installing Norton Personal Firewall, take a moment to review the system requirements.

Versions of Norton Personal Firewall for both Mac OS 8.1 to 9.x and Mac OS X are included on the CD. For instructions on installing and using Norton Personal Firewall for Mac OS 8.1 to 9.x, see the *Norton Personal Firewall User's Guide* PDF in the Install for Mac OS 9 folder on the CD.

System requirements

Norton Personal Firewall does not support Mac OS X versions 10.0 to 10.1. If you want to install Norton Personal Firewall on Mac OS X, you must upgrade to at least version 10.1.5.

- Macintosh OS X 10.1.5 or later
- G3 or G4 processor
- 128 MB of RAM
- 30 MB of available hard disk space for installation
- CD-ROM or DVD-ROM drive
- Internet connection

Before installation

The Read Me file on the Norton Personal Firewall for Macintosh CD contains late-breaking information and installation troubleshooting tips, which you should read before you install Norton Personal Firewall.

Read the Read Me file

The Read Me file contains a summary of what's new and changed in Norton Personal Firewall, along with condensed versions of key procedures and technical tips.

To read the Read Me file

1. Insert the Norton Personal Firewall for Macintosh CD into your CD-ROM drive.
2. In the CD window, open the **Install for Mac OS X** folder.
3. Double-click the **Read Me** file.

Installation

Install Norton Personal Firewall from the Norton Personal Firewall for Macintosh CD.

Norton Personal Firewall for Mac OS X protects both Mac OS X and Classic.

The installation procedure requires that you enter an Administrator password. If you do not know if your login is an Admin login, you can check it in System Preferences.

To check your login type

1. On the Apple menu, click **System Preferences**.
2. Do one of the following:
   - In Mac OS X version 10.2 and later, click **Accounts**.
   - In Mac OS X version 10.1.5, click **Users**.

   Your login name and type are listed.

To install Norton Personal Firewall for Macintosh

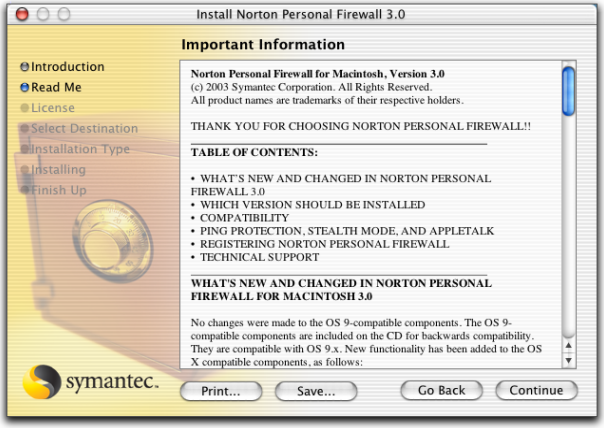
1. Insert the Norton Personal Firewall for Macintosh CD into the CD-ROM drive.
   If the CD window doesn't open automatically, double-click the CD icon to open it.
2. In the CD window, open the **Install for Mac OS X** folder.

3 Double-click **Install Personal Firewall**.

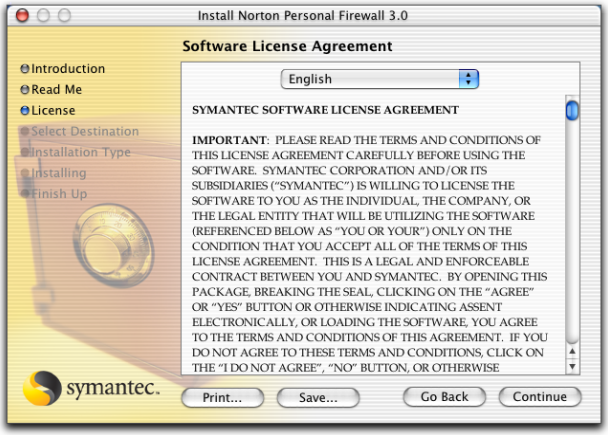
If you are installing Norton Personal Firewall on Mac OS X 10.1.5, the Authenticate window does not automatically appear. Click the lock in the lower-left corner of the Authorization window to open the Authenticate window and continue with the rest of the procedure.

4 In the Authenticate window, type your Administrator password, then click **OK**.

5 In the Welcome to the Norton Personal Firewall 3.0 Installer window, click **Continue**.

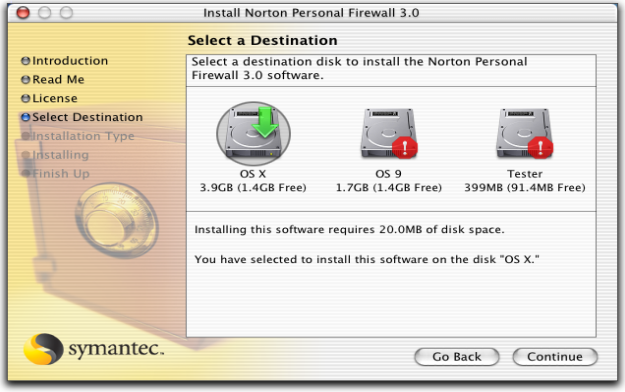

Install Norton Personal Firewall 3.0
Important Information
Introduction
Read Me
License
Select Destination
Installation Type
Installing
Finish Up
Norton Personal Firewall for Macintosh, Version 3.0
(c) 2003 Symantec Corporation. All Rights Reserved.
All product names are trademarks of their respective holders.
THANK YOU FOR CHOOSING NORTON PERSONAL FIREWALL!!
TABLE OF CONTENTS:
• WHAT'S NEW AND CHANGED IN NORTON PERSONAL FIREWALL 3.0
• WHICH VERSION SHOULD BE INSTALLED
• COMPATIBILITY
• PING PROTECTION, STEALTH MODE, AND APPLETALK
• REGISTERING NORTON PERSONAL FIREWALL
• TECHNICAL SUPPORT
WHAT'S NEW AND CHANGED IN NORTON PERSONAL FIREWALL FOR MACINTOSH 3.0
No changes were made to the OS 9-compatible components. The OS 9-compatible components are included on the CD for backwards compatibility. They are compatible with OS 9.x. New functionality has been added to the OS X compatible components, as follows:
symantec.
Print...
Save...
Go Back
Continue

6 Review the Read Me text, then click **Continue**.

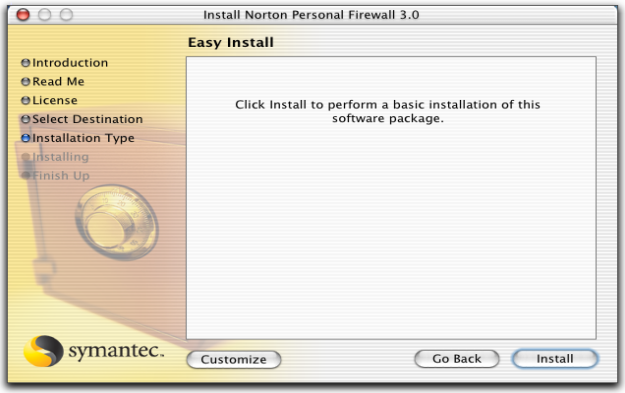

Install Norton Personal Firewall 3.0
Software License Agreement
Introduction
Read Me
License
Select Destination
Installation Type
Installing
Finish Up
English
SYMANTEC SOFTWARE LICENSE AGREEMENT
IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE
symantec.
Print...
Save...
Go Back
Continue

7 In the Software License Agreement window, click **Continue**.

8 In the agreement dialog box that appears, click **Agree**.
If you disagree, you cannot continue with the installation.



9 Select the disk on which you want to install Norton Personal Firewall, then click **Continue**.



10 In the installation type window, do one of the following:

- For a full installation, click **Install**. (If you have other Symantec products installed on your computer, this button may say Upgrade.)
- To see a list of components being installed, click **Customize**. When you have finished reviewing the list, click **Install**.

11 In the verification dialog box, click **Continue Installation**.

12 Choose whether or not you want to run LiveUpdate to ensure that your software is up-to-date.

13 When installation is complete, click **Restart**.

After installation

Now that you've installed Norton Personal Firewall, you have the following options:

Task	More information
Restart your computer.	See "Restart your computer" on page 18.
Register your software.	See "Register Norton Personal Firewall" on page 19.
Check for late-breaking news about your new software. Use the Internet link installed in the Norton Personal Firewall folder.	See "Read Late Breaking News" on page 20.

Restart your computer

After you install Norton Personal Firewall and restart your computer, it is protected from intrusion. The Norton Personal Firewall extension loads each time that you start your computer and actively protects your computer unless you disable it.

If you cannot eject the CD

If you have trouble ejecting the CD after you restart your computer, try one of the following:

- Press the CD-ROM drive's eject button when your Macintosh restart chime sounds.
- On a Macintosh computer with a slot-loading CD-ROM drive, press and hold the mouse button while starting up to eject the CD.

Register Norton Personal Firewall

Using your existing Internet connection, you can register Norton Personal Firewall for Macintosh via the Internet.

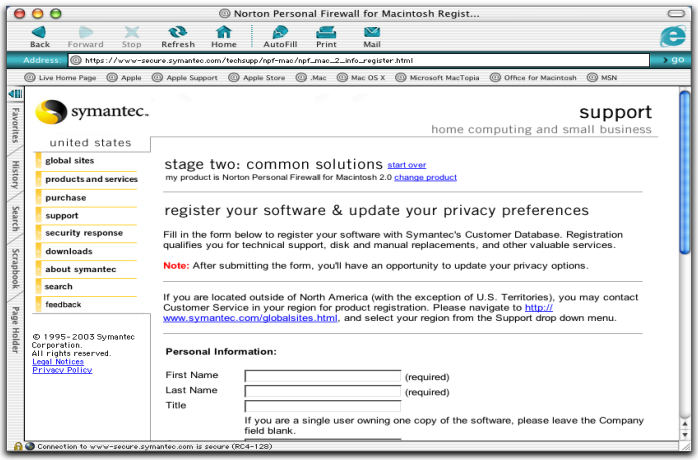
To register via the Internet

See "If you connect to the Internet through America Online" on page 20.

1. Connect to the Internet.
   If you use America Online (AOL) to connect to the Internet, you need to connect to it first.
2. In the Norton Solutions folder, double-click **Register Your Software**.

Your default Internet browser displays the Symantec support page.

3. On the support page, click **I am a home/small business user**.
4. On the register your software page, click **Norton Personal Firewall for Macintosh**.
5. Select the correct version of the product.
6. Click **continue**.



7. On the registration page for Norton Personal Firewall for Macintosh, type all of the required information.
8. Click **Submit Registration**.

Read Late Breaking News

Norton Personal Firewall for Macintosh installs a Late Breaking News link. Use this link to get the latest information available for your installed software.

To read Late Breaking News

See "If you connect to the Internet through America Online" on page 20.

1. Connect to the Internet.
   If you use America Online (AOL) to connect to the Internet, you need to connect to it first.
2. In the Norton Solutions folder, double-click **Late Breaking News**.

   Your default Internet browser displays the Symantec Macintosh products page.

If you connect to the Internet through America Online

If you use America Online (AOL) as your *Internet service provider* (ISP), you must connect to AOL before you go to the Symantec software registration page or view Late Breaking News.

To connect to the Symantec Web site through AOL

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Move the AOL browser and any other open AOL windows out of the way.
4. In the Norton Personal Firewall window, do one of the following:
   - Double-click **Register Your Software**.
     Continue with the registration procedure. See "Register Norton Personal Firewall" on page 19.
   - Double-click **Late Breaking News**.
     Continue with the procedure for reading the news. See "Read Late Breaking News" on page 20.
5. Disconnect from AOL.

If you need to uninstall Norton Personal Firewall

If you need to remove Norton Personal Firewall from your computer, use the Symantec Uninstaller on the Norton Personal Firewall for Macintosh CD. The process is faster if all other programs are closed before you uninstall Norton Personal Firewall.

The uninstall procedure requires that you enter an Administrator password. If you do not know if your login is an Admin login, you can check it in System Preferences.

To check your login type

1. On the Apple menu, click **System Preferences**.
2. Do one of the following:
   - In Mac OS X version 10.2 and later, click **Accounts**.
   - In Mac OS X version 10.1.5, click **Users**.

   Your login name and type are listed.

To uninstall Norton Personal Firewall

1. Insert the Norton Personal Firewall for Macintosh CD into the CD-ROM drive.
   If the CD window doesn't open automatically, double-click the CD icon to open it.
2. In the CD window, open the **Install for Mac OS X** folder.
3. Open the **UnInstall** folder.
4. Double-click **Symantec Uninstaller**.
5. In the Uninstall Symantec Products window, check **Norton Personal Firewall**.
6. Click **Uninstall**.
7. Confirm that you want to delete the product.
8. In the Authenticate window, type your Administrator password, then click **OK**.
9. In the window that displays the list of deleted items, click **Close**.
10. In the Uninstall Symantec Products window, click **Quit**.

Norton Personal Firewall basics

3

Norton Personal Firewall basics include general information about how to work with Norton Personal Firewall and how to access more information about it.

How to open and exit Norton Personal Firewall

You do not need to open Norton Personal Firewall for your computer to be protected. Protection is enabled upon startup after you have installed Norton Personal Firewall. You must specifically disable Norton Personal Firewall to interrupt protection.

To change or test your protection settings or review firewall activity, you need to open Norton Personal Firewall.

To open Norton Personal Firewall

1. On the menu bar, click the Norton QuickMenu icon.
2. On the Norton QuickMenu, click **Norton Personal Firewall > Open Norton Personal Firewall**.
3. If the Setup window does not appear, on the Tools menu, click **Setup**.

4 If you cannot see the entire Setup window, click the **Service settings** arrow to enlarge it.

The first time that you open the Setup window, the protection settings on the right side of the window may not appear. To see the settings for one of the services listed on the left side of the window, select it.

To exit Norton Personal Firewall

❖ On the Personal Firewall menu, click **Quit Personal Firewall**.

Check your firewall settings

Use the Setup Assistant to review your general firewall settings and, if necessary, change them.

To check your firewall settings

1 Open Norton Personal Firewall.
The first time that you open Norton Personal Firewall after installation, the Setup Assistant opens automatically.

2 If the Setup Assistant is not open, on the Tools menu, click **Setup Assistant**.

3 In the Setup Assistant Welcome window, click **Continue**.
If you have any Internet services running on your computer, the Access Settings window lists those services and indicates whether or not the firewall is set to allow access to them. It also gives you the option of being notified should your computer's settings conflict with the firewall's settings. For example, File Sharing access is denied by default. If you have chosen the notification option and you turn on File Sharing, Norton Personal Firewall asks if you want to allow access to it.

4 In the Access Settings window, change the settings as necessary.

5 Click **Continue**.
If you have chosen to allow access to active services, a second Access Settings window appears, giving you the option of limiting that access to computers on your local network.

6 Select whether or not you want to limit access, then click **Continue**.
The Protection Settings window shows whether your firewall is set for minimum, medium, or maximum protection, and shows how those levels are defined, based on which settings are on or off.

7 In the Protection Settings window, if desired, move the slider to change the protection level.

8 Click **Continue**.

9 In the last window, click **Done**.

If you want to review a more detailed list of your firewall settings, use the Summary report.

To review the Summary report

1 On the Reports menu, click **Summary**.

2 Select how you want to view the Summary report. Your options are:

Sort the list.	Click any of the column headings to sort by that column. To change the sort direction, click the sorting triangle on the right side of the column header. To restore the original order, click Restore Default Order.
Change a setting.	Double-click any entry on the Summary report to close the report and open the window in which you can change the setting.
Save the list as a text file.	Click Save to file. Specify a file name and location, then click Save.

3 Click **Close** when you are done.

Disable and enable firewall protection

When Norton Personal Firewall is installed, it is set to deny access to all *TCP/IP services*. For most users, these settings provide the protection they need without interfering with their work on the computer. You don't need to change any of the settings unless you have specific access rules that you want to define.

You can stop protection at any time by disabling Norton Personal Firewall. You can disable it for a specified period or until you restart it.

You can disable (or enable) Norton Personal Firewall from two places: the Setup window or the Norton QuickMenu.

To disable or enable Norton Personal Firewall from the Setup window

1 Open Norton Personal Firewall.

2 In the Setup window, do one of the following:

- To disable protection, uncheck **Enable Norton Personal Firewall**.
- To enable protection, check **Enable Norton Personal Firewall**.

3 If you unchecked Enable Norton Personal Firewall, verify that you want to disable the firewall.

4 Exit Norton Personal Firewall.

To disable or enable Norton Personal Firewall from the Norton QuickMenu

1. On the Finder menu bar, click the Norton QuickMenu icon.
2. On the Norton QuickMenu, click **Norton Personal Firewall**.
3. Select one of the following:
   - Disable firewall
   - Enable firewall

Disable Norton Personal Firewall temporarily

Use the Norton QuickMenu to disable protection for a specified time period.

To disable Norton Personal Firewall temporarily

1. On the Finder menu bar, click the Norton QuickMenu icon.
2. On the Norton QuickMenu, click **Norton Personal Firewall > Disable firewall temporarily**.
3. In the Temporarily Disable Firewall window, type the number of minutes for which you want Norton Personal Firewall to be disabled.
4. Click **Disable**.

Customize your toolbars

The Setup window, Access History log, and Connected Users report all have toolbars that you can customize to suit your needs.

To customize your toolbars

1. Open Norton Personal Firewall.
2. Open the window with the toolbar you want to change.
3. On the Window menu, click **Customize Toolbar**.
4. In the toolbar dialog box, drag the icons into and out of the toolbar at the top of the window until you have the set you want. You can change the location in which an icon appears by dragging it to the desired location.
5. If you want to return the toolbar to its original appearance, drag the default set of icons at the bottom of the dialog box to the toolbar.

6 By default, all icons appear with descriptive text. To change the default appearance, select one of the following:

- Icon & Text
- Icon Only
- Text Only

7 When the toolbar appears the way that you want it, click **Done**.

For more information

Norton Personal Firewall provides instructional material in three formats:

User's Guide	The User's Guide provides basic conceptual information and procedures for using all of the features of Norton Personal Firewall. Use the printed User's Guide if you cannot access the online material for any reason. Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help.
Built-in Help	Help includes all the material contained in the User's Guide, and a glossary for definitions of technical terms. Use Help to answer questions while you are using Norton Personal Firewall. See "Access Help" on page 28.
PDF	The PDF is an electronic version of the User's Guide that you can use if you prefer to look for information online in a book-like format or if you want to provide additional copies of the User's Guide. The PDF also includes a glossary for definitions of technical terms. See "Access the User's Guide PDF" on page 29.

In addition to this material, there is a Read Me file on the Norton Personal Firewall for Macintosh CD. Check the Read Me file before you install Norton Personal Firewall for late-breaking information.

Finally, you can always check the Symantec Web site for information about Norton Personal Firewall.

Access Help

Opening Help in Norton Personal Firewall displays the Apple Help Viewer with a list of Help topics.

To access Help

❖ On the Help menu, click **Personal Firewall Help**.

Tips for exploring Help:

- To search for a specific topic, in the search field at the top of the Help window, type the related term, then click Ask.
- Terms that are underlined and blue in the text are defined in the glossary. Click the word to go to its definition. Click the left-arrow button to return to the topic.
- Links to related topics appear at the end of a topic.
- Some topics include links that open the window in which you can begin the task described.

Access the User's Guide PDF

The User's Guide is available in printable Adobe Acrobat PDF format on the CD.

To open the PDF

1. Insert the Norton Personal Firewall for Macintosh CD into the CD-ROM drive.
2. In the CD window, double-click the **Install for OS X** folder.
3. In the Install for OS X folder, double-click the **Documentation** folder.
4. Double-click the **Norton Personal Firewall User Guide** PDF.

You can also drag the PDF to your hard disk.

Tips for exploring the PDF:

- When you open the PDF, the table of contents appears in the left margin. In the table of contents, click a heading to jump to that topic.
- To search for a specific topic, use the Find command on the Edit menu.
- Terms that are italicized and blue in the text are defined in the glossary. Click the word to go to its definition. Click Go to Previous View to return to the topic.

Open the Read Me file

The Read Me file on the Norton Personal Firewall for Macintosh CD contains information that was unavailable at the time that the User's Guide was published.

To open the Read Me file

1. Insert the Norton Personal Firewall for Macintosh CD into your CD-ROM drive.
2. In the CD window, open the **Install for Mac OS X** folder.
3. Double-click the **Read Me** file.

Explore the Symantec support Web site

The Symantec support Web site provides extensive information about Norton Personal Firewall. You can find updates, patches, Knowledge Base articles, and virus removal tools.

To explore the Symantec support Web site

1. On the Internet, go to www.symantec.com/techsupp
2. On the support Web page, under home/small business, click **Continue**.
3. On the home computing and small business Web page, click **start online support**.
4. Follow the instructions on the Web site to get the information you need.

If you cannot find what you are looking for using the online support pages, try searching the Web site.

To search the Symantec support Web site

1. On the left side of any Web page in the Symantec support Web site, click **search**.
2. In the Search text box, type a word or phrase that best represents the information for which you are looking.
   For tips on entering your search text, click **help** at the bottom of the page.
3. Check the area of the Web site that you want to search.
4. Click **search**.

Protecting disks, files, and data from intrusion

4

Norton Personal Firewall protects your computer from connections using the access settings that you specify. You can allow access for certain computers, listing them by *IP address*, and you can define additional *services* to protect on your computer.

What Norton Personal Firewall protects

Norton Personal Firewall protects your computer from outside intrusion through *TCP/IP* (Transmission Control *Protocol*/Internet Protocol) and, optionally, *UDP* (User Datagram Protocol) connections. This means that while you are connected to the Internet or another network, no computer can access the files, programs, or other information on your computer without your authorization. This authorization is granted to a computer, not to an individual user, so any user on that computer has access. You can also block *ICMP* requests.

Norton Personal Firewall cannot be used to control outgoing information. For example, you cannot use it to encrypt personal information such as a credit card number that you are providing to a Web site. It also does not block Bluetooth traffic. (Bluetooth technology provides wireless connections between digital devices that have been enabled for it. It is built into some Macintosh computers.)

Specify access by IP address or host name

See "Add IP addresses" on page 52.

When you allow or deny access for certain computers, you can list those computers by their Internet protocol (IP) addresses (protocols are sets of rules that govern data transmission). IP addresses consist of four numbers from 0 to 255, connected by periods such as 206.204.212.3. Every computer on the Internet has a unique IP address.

You may not know a computer's IP address, but you know its host name, the name that identifies a computer on a network. For example, www.symantec.com is the host name for the Symantec Web site. Host names are converted to IP addresses by the *Domain Name System* (DNS). You can enter either a host name or an IP address in an access list.

IP addresses can be specified individually, as a range beginning with a certain value, or as a range that corresponds to a subnet. A subnet is a local area network that is part of a larger intranet or the Internet.

Define protection for port numbers

See "Define a custom service to protect" on page 54.

You can list *IP addresses* to allow or deny access for each *service* on your computer. The most common services are already defined in the Setup window for you. For those not listed, you can create an entry in the services list by specifying its name and *port number*.

Internet services communicate by means of *ports*, with each service using a unique port number. For instance, Web Sharing usually uses port 80, and File Sharing over *TCP/IP* uses port 548. Sometimes services are run on alternate ports. If, for example, two Web servers (computers that deliver Web pages to your browser) were running on the same computer, they could not both use the same port number–one of them would be assigned an alternate port number. Specifying protection by port number is useful for creating protection for services not predefined by Norton Personal Firewall, and for creating protection for services that use alternate port numbers.

See "Enable UDP protection" on page 59.

You can also specify protection for services that use *UDP* ports. However, this feature is intended for use only by those who understand Internet *protocols* well, as denying access to the wrong UDP ports can prevent your computer from functioning correctly on the Internet.

Track access attempts

Norton Personal Firewall records complete information about access attempts to your computer. It can log all denied accesses, allowed accesses, or both, and can provide you with immediate notification of allowed or denied accesses.

Norton Personal Firewall and AppleTalk

There are two principal network *protocols* used on Macintosh computers: *AppleTalk* and *TCP/IP*. AppleTalk provides local *services* that are not available over the Internet such as printing, sharing files with other computers on the same network, and company-specific applications. TCP/IP provides Internet services such as email and access to Web sites, as well as File Sharing and program linking over the Internet or an intranet.

TCP/IP security on Norton Personal Firewall

Norton Personal Firewall adds a level of protection to any application that uses the TCP *protocol* by granting access only for limited sets of computers on the Internet, based on their *IP addresses*. For example, if you have enabled File Sharing over *TCP/IP*, you must also grant File Sharing access in Norton Personal Firewall. You can either allow all access in Norton Personal Firewall or you can allow access only for certain IP addresses.

In Mac OS X, *AppleTalk* uses TCP/IP to connect to File Sharing and program linking *services* on other Mac OS X computers. Because of this, Norton Personal Firewall detects these connections and blocks them if you have not specifically allowed access.

See "Customizing firewall protection" on page 51.

To avoid blocking AppleTalk, set up File Sharing and program linking access in Norton Personal Firewall to allow access to those computers to which you connect using AppleTalk.

Monitoring access attempts

5

Norton Personal Firewall logs all incoming access attempts, whether they are allowed or denied. You can also choose to log outgoing access attempts. Use this log to verify that Norton Personal Firewall is working correctly.

Monitor firewall activity

When Norton Personal Firewall is installed, it is set to log both denied and allowed incoming access attempts. These attempts appear in the Access History log, which you can view at any time.

You may want immediate notification of access attempts under certain circumstances. For example, when you first install Norton Personal Firewall, you may want to evaluate every access attempt to ensure that Norton Personal Firewall is working. You may also want to receive immediate notification if you have changed some settings and want to make sure that they have produced the results that you want.

See "Test firewall settings" on page 37.

To verify protection settings or changes to those settings before going online, use the Norton Personal Firewall Quick Check feature. Quick Check simulates a TCP connection, logs an access attempt, and triggers a notification if you have enabled that feature.

You can also test your computer's security through a link to the Symantec Security Check Web site. You can use the results of the test to determine if your firewall settings are adequate.

Once you have set up your firewall, you can check to see if you are getting the desired results by reviewing the Connected Users report. If you have set your firewall to block all connections, this report should be empty. If you have set your firewall to allow certain users to connect to your computer, you can use this report to verify that they are able to connect.

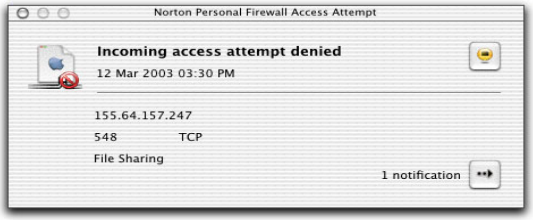
Enable or disable notification of access attempts

See "About alert messages" on page 40.

For both incoming and outgoing connections, you can choose to be notified of all denied access attempts, all allowed access attempts, or both. If you have enabled notification, an *alert* appears every time an access attempt of the kind specified occurs.

You can also choose to be notified if your computer's settings conflict with the firewall's settings. For example, you may have all access to File Sharing blocked in Norton Personal Firewall, then enable File Sharing in System Preferences. Because the firewall is blocking access, File Sharing is effectively unusable. Norton Personal Firewall can alert you of this conflict and change the firewall settings for you.

Access notification options can be set individually for any *service* that is listed in the Setup window. Any service for which individual notification options have not been set uses the global options that are set in Preferences.



Enabling or disabling notification has no effect on logging. Also, disabling logging has no effect on notification, although the notification alert is your only record of the access attempt.

To enable or disable access notification for a service

1. Open Norton Personal Firewall.
2. In the Setup window, select the service for which you want to set notification options.
3. Click **Edit**.
4. In the server setup dialog box, click **Notifications**.
5. Specify the desired notification options.
6. Click **Save**.

To enable or disable global access notification

1. Open Norton Personal Firewall.
2. On the Personal Firewall menu, click **Preferences**.
3. In the Personal Firewall Preferences window, click **Notifications**.
4. Specify the desired notifications options.
5. Close the Preferences window.
   Your changes are automatically saved.

Test firewall settings

You can test your firewall settings in two ways: using the Quick Check option to simulate access to a *service*, or using the Security Check option to connect to the Symantec Web site and scan your computer for vulnerability to Internet *threats*.

Simulate access with Quick Check

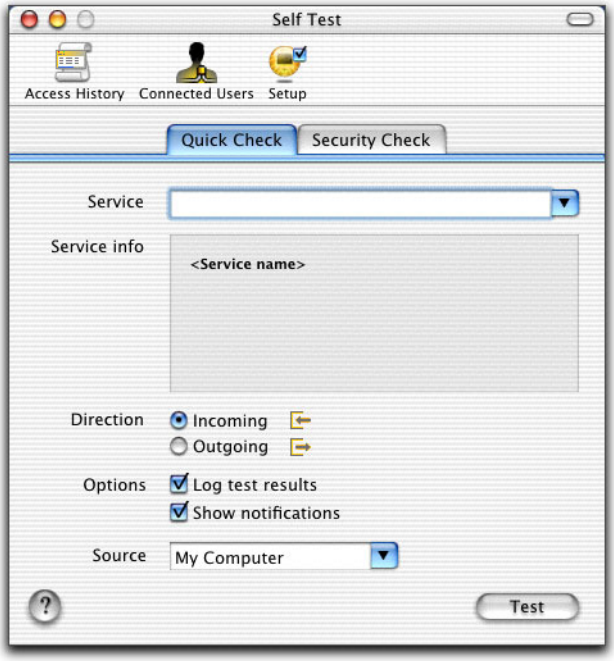
By default, the Quick Check option uses the *IP address* of your computer to simulate access to one of the services listed in the Setup window. You can also specify an IP address to use in the test. If your computer does not have an IP address, you must connect to the Internet before using Quick Check.

Norton Personal Firewall must be enabled for Quick Check to work.

To simulate access with Quick Check

1. Open Norton Personal Firewall.
2. On the Tools menu, click **Self Test**.

3 In the Self Test window, click **Quick Check**.



4 Select a service to test.
The protection defined for the specified service appears under the service name.

5 Under Direction, select one of the following:

- Incoming
- Outgoing

6 Under Options, select where you want the test results to appear. Your options are:

Log test results	The access attempt appears in the Access History log.
Show notifications	The access attempt appears in the Recent access attempts menu option in the Dock menu.

You can select either, both, or neither. The test results always appear in the Self Test window.

7 To specify an IP address other than your computer's, in the Source field, type the desired IP address.

8 Click **Test**.

Scan for vulnerabilities with Symantec Security Check

Use Symantec Security Check to test your computer's vulnerability to security intrusions. The Symantec Security Check link in Norton Personal Firewall connects you to the Symantec Web site. The Web site contains detailed information about what Symantec Security Check scans for and provides instructions for running the scan.

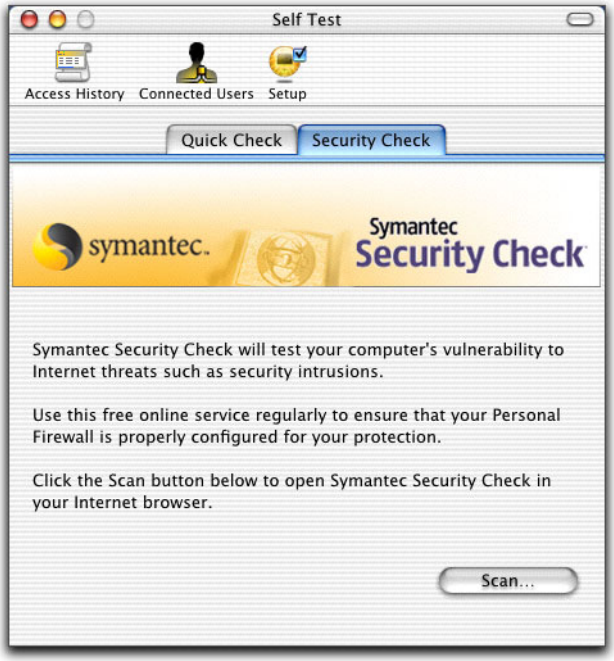
If your computer resides behind a corporate firewall, Symantec Security Check can give incorrect results.

To scan for vulnerabilities with Symantec Security Check

1 Open Norton Personal Firewall.

2 On the Tools menu, click **Self Test**.

3 In the Self Test window, click **Security Check**.


Self Test
Access History
Connected Users
Setup
Quick Check
Security Check
symantec.
Symantec
Security Check
Symantec Security Check will test your computer's vulnerability to Internet threats such as security intrusions.
Use this free online service regularly to ensure that your Personal Firewall is properly configured for your protection.
Click the Scan button below to open Symantec Security Check in your Internet browser.
Scan...

4 Click **Scan**.
Your browser opens on the Symantec Security Check Web page.

5 To learn more about what Security Check does, on the Security Check Web page, click **About Scan for Security Risks**.

6 To run the scan, click **Scan for Security Risks**.

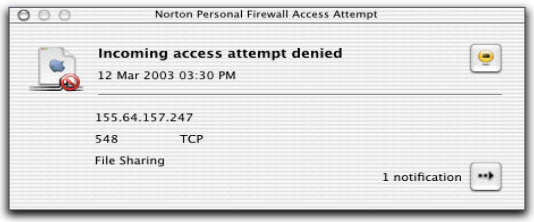
When the scan is complete, the results page lists all the areas checked and your level of vulnerability in each one. For any area marked as at risk, you can get more details about what the problem is and how to fix it.

Respond to access attempts

View the Access History log occasionally to check for any unusual activity or problem such as denied access for someone who should have access.

About alert messages

If you have enabled notification of access attempts, an *alert* window appears on your screen when access attempts occur. The number of alerts that you have received is indicated in the lower-right corner of the alert window. You can review the alerts by clicking the right arrow.



Alerts contain details of access attempts. If an access attempt seems suspicious, view the Access History log.

View the Access History log

All logged access attempts appear in the Access History log. Use this log of access attempts to spot potential security violations. When reading it, check for patterns such as:

- Many denied accesses, especially from a common client *IP address*
- Sequences of *port* numbers from the same client IP address, possibly indicating a port scan (someone trying many ports on your computer, looking for one that can be accessed)

It is normal to see some denied access attempts on a random basis (not all from the same IP address, and not to a sequence of port numbers). In some cases, access attempts are made due to activity on your own computer such as connecting to an *FTP* server and sending email.

To view the Access History log

1. Open Norton Personal Firewall.
2. On the Reports menu, click **Access History Log**.

Access History contents

The type of accesses being logged appears at the top of the window. The fields included in the window are as follows.

Date & Time	The date and time of the access attempt.
Action	Whether the access attempt was allowed or denied.
Direction	Whether the access attempt was incoming or outgoing.
Address	The IP address of the computer to or from which access was attempted.

Service	The name, if any, of the Internet service to or from which access was attempted.
Port	The port number to or from which access was attempted.
Mode	The communication mode over which the access attempt was made. Possible modes are TCP, UDP, and ICMP.
Type	The reason the entry appears in the log.
Host	The host name of the computer to or from which access was attempted. If the host name cannot be determined, the computer's IP address appears instead.

Access attempts with a blue dot in the first column occurred within the previous 15 minutes.

Change the appearance of the Access History log

You can change the appearance of the Access History log to suit your needs.

To change the appearance of the Access History log

❖ Customize the Access History log as desired. Your options are:

Sort by column.	Click the header of the column that you want to sort by. To change the sort direction, click the sorting triangle on the right side of the column header. By default, the log is sorted by date, with the most recent entries at the end.
Rearrange the columns.	Drag the column headings to the positions in which you want the columns to appear.
Resize the columns.	Drag the edge of the column heading until the column is the size that you want.
Remove columns.	On the Reports menu, click View options to get a list of the columns displayed. Uncheck the columns that you don't want to see, then click Save.

Export the Access History information

The contents of the Access History log can be exported to a tab-delimited text file. You can export the entire log or selected entries in the log. The Access History log must be open to export it.

To export the Access History information

1. On the Reports menu, click **Access History Log**.
2. If desired, select individual entries to export.
3. On the File menu, click **Export**.
4. In the export dialog box, specify a name and location for the file.
5. If you are exporting selected entries, check **Export only selected entries**.
6. Click **Save**.

Clear the Access History log

If the list in the Access History log gets too long, you can clear the log.

To clear the Access History log

1. On the Reports menu, click **Access History Log**.
2. On the Edit menu, click **Clear Log**.
3. Verify that you want to clear Access History.

Learn more about a specific access attempt

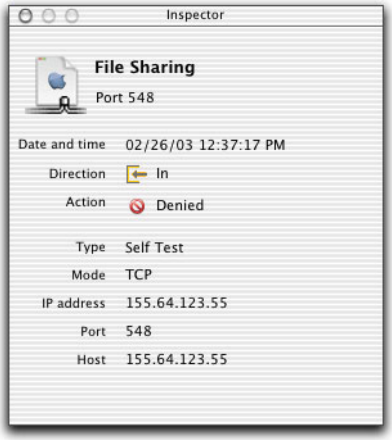
You can get more information on any entry in the Access History log from the Inspector window, the Learn More Web site, or the Visual Tracking Web site.

Open the Inspector window

The Inspector window gives you all of the Access History log information about an access attempt in one window.

To open the Inspector window

❖ In the Access History log, double-click the line for which you want more information.



Access the Learn More Web site

The Norton Personal Firewall Learn More Web site displays more details about the access attempt and provides links to other sites that may provide details about the source (the Host Name field) of access attempts.

To access the Learn More Web site

1 In the Access History log, select the access attempt for which you want more information.

2 On the Tools menu, click **Learn More**.

Access the Visual Tracking Web site

The Visual Tracking Web site shows you a map with the location of the owner of the *IP address* that is the source of an access attempt. It also gives you the name of the IP address' Internet service provider and links to more details about the owner of the IP address.

To access the Visual Tracking Web site

1 In the Access History log, select the access attempt for which you want more information.

2 On the Tools menu, click **Visual Tracking**.

Change logging preferences

Logging of all incoming access attempts and suspicious activity is enabled by default. Keep these settings until you feel confident that your configuration of Norton Personal Firewall is working as you planned. Logging all accesses can create a large log file quickly, so you may eventually want to limit what is being logged.

You may also want to log access attempts to or from some *services* and not others. You can define what gets logged for each service if desired. If you do not define individual logging settings for a service, the settings specified in Preferences are used.

To change default logging preferences

1. Open Norton Personal Firewall.
2. On the Personal Firewall menu, click **Preferences**.
3. In the Personal Firewall Preferences window, click **Logging**.
4. Specify Logging options.
5. Close the Preferences window.
   Your changes are automatically saved.

To define logging preferences for a service

1. Open Norton Personal Firewall.
2. In the Setup window, select the service for which you want to define logging preferences.
3. Click **Edit**.
4. In the service setup dialog box, click **Logging**.
5. Specify your logging preferences for the service.
6. Click **Save**.

Disable logging

Logging and *service* protection are independent of one another. For example, if you are logging allowed accesses and then make Norton Personal Firewall inactive, Norton Personal Firewall continues logging and logs all accesses, since all accesses are allowed. Under certain circumstances such as when you want to create a new log file, you need to disable logging altogether. Disabling logging has no effect on Norton Personal Firewall protection.

If you have set individual logging preferences for a service, you must disable those settings also to completely stop all logging.

To disable default logging options

1. Open Norton Personal Firewall.
2. On the Personal Firewall menu, click **Preferences**.
3. In the Personal Firewall Preferences window, click **Logging**.
4. Uncheck all logging options.
5. Close the Preferences window.
   Your changes are automatically saved.

To disable logging for a service

1. Open Norton Personal Firewall.
2. In the Setup window, select the service for which you want to disable logging.
3. Click **Edit**.
4. In the service setup dialog box, click **Logging**.
5. Uncheck all logging options.
6. Click **Save**.

How the log file is structured

The log file is a tab-delimited text file named Norton Personal Firewall Log. It can be read by any word processor or spreadsheet application, or by some log-analyzer applications.

The log file is located in Library:Application Support:Norton Solutions Support:Norton Personal Firewall.

Access attempts are logged using the following tokens (which are included in the !!LOG_FORMAT line whenever Norton Personal Firewall starts or a new log file is written):

DATE	Date, time, and time zone of access attempt
RESULT	OK for an allowed access; ERR! for a denied access
HOSTNAME	IP address of the client attempting access to the given port
SERVER_PORT	The port to which access is attempted by the given client

METHOD	The protocol used by the access attempt (TCP or UDP)
DIRECTION	IN for incoming access attempts; OUT for outgoing access attempts
TYPE	Reason that the entry appears in the log

Exporting the log file to a spreadsheet and sorting the data may make it easier to spot patterns that could indicate a potential security violation. For example:

- Sort by the RESULT field and then by HOSTNAME. In the rows containing ERR! in the RESULT field, look for groupings of *IP addresses* in the HOSTNAME field. Large numbers of ERR! lines for a given IP address may indicate an attempted security breach.
- Sort by RESULT, then by HOSTNAME, and then SERVER_PORT. In the rows containing ERR! in the RESULT field, look for sequences of *port* numbers in the SERVER_PORT field that have the same IP address in the HOSTNAME field. Sequences of port numbers from a given IP address may indicate a port scan.

See "To view the Access History log" on page 41.

For information on an IP address in the log file (or in a notification *alert*), refer to the Access History log.

Work with the Connected Users report

The Connected Users report lists all of the computers that are currently connected to your computer. If a computer has made multiple connections, all of those connections are listed separately. You can use the Connected Users report to verify that those users who should be connected to your computer are able to do so and that no one who should be blocked is getting through.

While viewing the Connected Users report, you can add the *IP address* of a connected computer to a deny or allow access list, disconnect the computer from your computer, get more information about the connected computer, and export the list to a text file.

To review the Connected Users report

1 Open Norton Personal Firewall.

2 On the Reports menu, click **Connected Users**.
The Connected Users report displays:

Recent connection	A blue dot appears in the first column if the connection was made within the last 15 minutes.
Connection status	In the second column, a green dot appears if the user is currently connected. A red dot appears if you disconnected the user.
Connection start time	The time that the connection was made.
Service	The service through which the connection was made.
Address	The IP address of the computer that is making the connection.
Application	The application that is used to make the connection.
Host	The host name of the connected computer. If the host name cannot be determined, the computer's IP address appears instead.

Change the appearance of the Connected Users report

You can change the appearance of the Connected Users report to suit your needs.

To change the appearance of the Connected Users report

❖ Customize the Connected Users report as desired. Your options are:

Sort by column.	Click the header of the column that you want to sort by. To change the sort direction, click the sorting triangle on the right side of the column header. By default, the report is sorted by connection start time, with the most recent entries at the end.
Rearrange the columns.	Drag the column headings to the positions in which you want the columns to appear.

Resize the columns.	Drag the edge of the column heading until the column is the size that you want.
Remove columns.	On the Reports menu, click View options to get a list of the columns displayed. Uncheck the columns that you don't want to see, then click Save.

Disconnect a connected user

See "Change the time limit for disconnected users" on page 50.

You can disconnect any user who is listed in the Connected Users report. When you do so, the user is prevented from reconnecting to your computer for 30 minutes, by default. You can change this time limit in Preferences.

Some *services* make more than one connection. For example, *FTP* often makes two connections and some Web browsers can make up to eight. All of these connections appear in the report separately as duplicate entries, but disconnecting one of the duplicate entries disconnects them all.

To permanently prevent users from reconnecting to your computer, add their *IP addresses* to your deny access list for that service.

To disconnect a connected user

1. In the Connected Users report, select the computer that you want to disconnect.
2. On the toolbar, click **Disconnect User**.
3. In the confirmation dialog box, click **Disconnect**.

Get more information about a connected user

More information about a connected user is available from the following places:

Show Info window	The Show Info window gives you all of the Connected Users report information about the connection in one window.
Learn More Web site	The Norton Personal Firewall Learn More Web site displays more details about the connected user and provides links to other sites that may provide details about the source of the connection.
Visual Tracking Web site	The Visual Tracking Web site shows you a map with the location of the owner of the IP address listed in the report. It also gives you the name of the IP address' Internet service provider and links to more details about the owner of the IP address.

To get more information about a connected user

1. In the Connected Users report, select the connection for which you want more information.
2. On the toolbar, select one of the following:
   - Show Info
   - Learn More
   - Visual Tracking

Export the Connected Users list

You can export the contents of the Connected Users report to a text file.

To export the Connected Users list

1. On the toolbar of the Connected Users report, click **Export List**.
2. In the Save as dialog box, type the name under which you want the report to be saved.
3. Select the location in which you want the report to be saved.
4. Click **Save**.

Change the time limit for disconnected users

When you disconnect a user from the Connected Users report, that user cannot reconnect to your computer for the amount of time that is specified in Preferences.

To change the disconnect users time limit

1. Open Norton Personal Firewall.
2. On the Personal Firewall menu, click **Preferences**.
3. In the preferences window, click **Connected Users**.
4. Change the amount of time that the user must remain disconnected as desired.
5. Close the preferences window.
   Your changes are automatically saved.

Customizing firewall protection

6

As you work with Norton Personal Firewall, you may need to adjust your access settings. For example, you may want to allow File Sharing for a colleague working at another location. You may also find a *service* on your computer that is not listed separately in the Setup window and requires customized protection. You can add that service to the list. You can also extend protection to your computer's *UDP ports*.

See "Disconnect a connected user" on page 49.

Changes to access settings do not affect computers that are connected to your computer when you make the changes. When the connection is broken, the changes take effect. For example, if a computer is connected to File Sharing on your computer and you deny File Sharing access, the computer remains connected until either the user logs off or you explicitly break the connection.

Set protection for standard Internet services

The Internet *services* built into the Macintosh OS are defined in the Setup window of Norton Personal Firewall. Services that are not listed are protected using the settings for the All Others service entry. They are all set to deny all access by default. You can change protection settings for any of the services listed.

For every service listed in the Setup window, for both incoming and outgoing connections, you can:

- Deny all access.
- Allow access to addresses in the list.
- Deny access to addresses in the list.
- Allow all access.

These settings are listed in order from most to least restrictive.

To deny or allow all access to a service

1. Select the service to which you want to deny or allow all access.
2. Select incoming or outgoing connections.
3. Select the option that you want.

See "Work with the Connected Users report" on page 47.

If you deny access to a service to which someone is connected, that change does not take effect until the connection is broken. You can see who is connected to a service on the Connected Users report.

To deny or allow access to a list of IP addresses

1. Select the service to which you want to deny or allow access.
2. Select incoming or outgoing connections.
3. Select the option that you want.
4. Define the IP addresses to go in the list.

See "Work with the Connected Users report" on page 47.

If you deny access to an *IP address* that is currently connected, that change does not take effect until the connection is broken. You can see the IP addresses currently connected to your computer on the Connected Users report.

To define a list of addresses to which to allow or deny access

1. Select the Internet service for which you want to define access.
2. Select incoming or outgoing connections.
3. Select whether you want to allow or deny access for a list of IP addresses.
4. Click **New** to add an address or range of addresses to the list.

Add IP addresses

You can add a single *IP address* or range of addresses to the allow or deny access list. When you add a range of addresses, you enter only the beginning of the range. Norton Personal Firewall determines the end of the range based on how much of the beginning IP address you enter.

To add a single address

1. In the address setup dialog box, in Allow access to, click **a single address**.
2. In the Address field, type the IP address or host name.
   To choose a computer on your network, click **Browse**.
3. Click **Save**.
   The address appears in the Setup window in the list.

To add a range of addresses

1. In the address setup dialog box, in Allow access to, click **addresses starting with**.
2. In the Base IP address field, type enough of an address to get the range of addresses that you want.
   As you enter each digit of a Base IP address, Norton Personal Firewall determines the end of the range and displays it in the Addresses range area of the address setup dialog box.
3. Click **Save**.

Add subnet addresses

You can add your own *subnet* or a different subnet to your deny or allow access list. If you use your own subnet, the *subnet mask* is filled in automatically. If you specify a different subnet, you must provide its subnet mask.

To add addresses for your own subnet

1. In the address setup dialog box, in Allow access to, click **all computers on a network**.
2. Click **Use My Subnet**.
   The base IP address and subnet mask for your subnet are filled in automatically.
3. Click **Save**.

To add addresses for a subnet other than your own

1. In the address setup dialog box, in Allow access to, click **all computers on a network**.
2. Type the base IP address and the subnet mask for the subnet into the appropriate fields.
3. Click **Save**.

Define a custom service to protect

You can add *services* that are not listed in the Setup window. You can select from a list of predefined services or enter your own.

To define a custom service

1 Under the services list, click **New**.

Name:
Description:
Ports
Logging
Notifications
New
Edit...
Delete
These are the ports that are used by this service. To add a port to the list, click the New button.
You can only add a new port to services you have created. You cannot modify services pre-defined by Norton Personal Firewall.
Cancel
Save

2 Select a service name. If the service that you want to add does not appear in the list, type it in the Name field.
If you select a service from the list, the port number appears automatically.

3 If desired, type a description of the service.

4 If you need to define a range of ports for the service, or if you typed a service name, click **New** to specify the port number or range.
An icon for the service appears automatically.

5 You can change the icon by copying and pasting or dragging and dropping the desired icon over the icon in the New Service dialog box.

6 If you want to specify logging or access notification preferences for this service that are different from the default preferences, do so on the Logging and Notification tabs. See "Enable or disable notification of access attempts" on page 36 and "Change logging preferences" on page 45.

7 Click **Save**.
The new service appears in the Setup window in the list. To specify access for that service, see "Set protection for standard Internet services" on page 51.

Edit or delete a custom service

For predefined *services*, you can only edit logging and notification settings. You cannot delete predefined services. You can edit or delete a custom service that you added to the list.

You cannot change the *port* number when editing the custom service. To change the port number, delete the service and add a new one with the correct port number.

To edit a custom service

1. In the Setup window, select the service that you want to edit.
2. Click **Edit**.
3. In the service setup dialog box, make the changes you desire.
4. Click **Save**.

To delete a custom service

1. In the Setup window, select the service that you want to delete.
2. Click **Delete**.
3. In the warning dialog box that appears, verify that you want to delete the service.

Change protection settings

You can make changes to the protection settings for a *service* at two levels. You can change the level of restriction (for example, from Deny all access to Allow access from only addresses in list) or you can change the list of addresses associated with a restriction level. You make these changes in the Setup window.

If you make a change to a service's protection settings that denies access to someone who is currently connected to that service, the change does not take effect until that person is disconnected from that service, either by logging off or by you breaking the connection.

Change the level of restriction

You can change the level of restriction for a *service* at any time.

To change the level of restriction

1. In the Setup window, select the service that you want to change.
2. Select incoming or outgoing connections.
3. Select the new restriction option:
   - If you are changing to a restriction option that refers to a list of IP addresses, you must create that list. See "Set protection for standard Internet services" on page 51.
   - If you are changing to either Deny all access or Allow all access from an option for which you have specified a list of IP addresses, you do not need to delete those addresses. They remain visible but unavailable in the Setup window.

Change an IP address list

For either restriction option requiring an *IP address* list, you can add to the list, edit the addresses in the list, or delete addresses from the list in the Setup window.

Before changing a list, make sure that the list you want to change is displayed by clicking the appropriate *service* and the correct connection direction.

To add an IP address to a list

1. In the Setup window, click **New**.
2. Add IP addresses as necessary.
3. Click **Save**.

To edit an IP address or range of addresses in a list

1. In the Setup window, select the address or range of addresses.
2. Click **Edit**.
3. In the IP address setup dialog box, make the changes that you want.
4. Click **Save**.

To delete an IP address from a list

1. In the Setup window, select the address or range of addresses.
2. Click **Delete**.

About active FTP support

Norton Personal Firewall provides active *FTP* support, which allows *downloading* of files from an FTP server without blocking the connection.

Active FTP support is on by default. If you use your computer as an FTP server, or if you want to block your computer from downloading files using FTP, you can turn off active FTP support.

To turn off active FTP support

1. Open Norton Personal Firewall.
2. On the Tools menu, click **Protection settings**.
3. In the protection settings dialog box, click **Custom Setup**.
4. Uncheck **Enable Active FTP support**.
5. Click **Save**.

Stealth mode

Usually, when an attempt to access your computer is denied by Norton Personal Firewall, a message is returned to the requesting computer indicating the denial. If you check Enable Stealth mode, no message is sent, thereby making your computer invisible to whoever tried to access it.

What Stealth mode does

When you enable Stealth mode, TCP, *UDP*, and almost all *ICMP* requests directed at *services* to which you have denied access are ignored. The exceptions are ICMP types 0 (echo replies for Pings sent), 3 (destination unreachable), and 11 (time exceeded). In addition, your computer is hidden from traceroute utilities. (Traceroute utilities are used to find the path that a *packet* takes from one computer to another.) Enabling Stealth mode also causes the ICMP messages to be logged in Access History.

You can also choose to enable Stealth mode for Rendezvous networking traffic. Doing so blocks all Rendezvous-based communications.

Disable Stealth mode

Stealth mode is enabled by default. Unless you have experienced problems such as *denial-of-service attacks*, you may want to disable it, as *ICMP* messages have legitimate uses on networks and for File Sharing.

To disable Stealth mode

1. Open Norton Personal Firewall.
2. On the Tools menu, click **Protection settings**.
3. In the protection settings dialog box, click **Custom Setup**.
4. Uncheck **Enable Stealth mode**.
5. Click **Save**.

Block suspicious activity

Suspicious activity is defined by Norton Personal Firewall as transmission of data *packets* whose source *IP addresses* are spoofed (made to look like those from a trusted host).

You can protect against both outgoing and incoming suspicious activity. Outgoing suspicious activity protection prevents your computer from spreading a malicious attack to other computers. Incoming suspicious activity protection blocks those kinds of attacks from reaching your computer.

To block suspicious activity

1. Open Norton Personal Firewall.
2. On the Tools menu, click **Protection settings**.
3. In the protection settings dialog box, click **Custom Setup**.
4. Check **Enable suspicious activity protection**.
5. Select whether you want to deny outgoing suspicious traffic, incoming suspicious traffic, or both.
6. Click **Save**.

About UDP

User Datagram Protocol (*UDP*) is a relatively simple *protocol* used for Internet operations. For example, the *Domain Name System* (DNS), which translates *host names* into *IP addresses*, uses UDP.

There is little reason to protect UDP *ports*. However, if you have a specific reason for protecting a UDP port, protect it with caution. Denying access to UDP *services* can cause problems when accessing the Internet.

Enable UDP protection

In most cases, you will want to protect only *UDP ports* up through 1023. These low-numbered UDP ports are used for standard *services* such as *DHCP* (Dynamic Host Configuration *Protocol*), commonly used to obtain a computer's *IP address*, and NTP (Network Time Protocol), which can be used by the Date & Time Control Panel. Higher-numbered ports are used dynamically by certain UDP services such as *DNS*. Denying access to high-numbered ports disables such services, since there is no way to know which port will be used by a given service.

To further avoid problems if you enable UDP protection, you can allow access to essential services. Choosing this option means that services such as DHCP and DNS can continue unimpeded.

To enable UDP protection

1. Open Norton Personal Firewall.
2. On the Tools menu, click **Protection settings**.
3. In the protection settings dialog box, click **Custom Setup**.
4. Check **Enable UDP protection**.
5. Check the other UDP options as desired. Your options are:
   - Protect outgoing UDP connections
   - Allow access to essential services
   - Protect all or a range of UDP ports
6. Click **Save**.

How UDP protection works

Once you enable *UDP* protection, it works much like TCP protection. Norton Personal Firewall uses the same *service* list for UDP as it does for TCP. Normally, a service uses either a TCP or a UDP *port*, but Norton Personal Firewall protects both types of ports for a given service (if UDP protection for that port is active).

One way that UDP protection differs from TCP protection is that UDP is a connectionless *protocol* (does not require a connection to send a message), while TCP is a connection-based protocol (requires a connection before sending messages). With TCP, Norton Personal Firewall can allow or deny only the connection attempt, and not the information following the attempt. With UDP, Norton Personal Firewall must allow or deny every piece of information destined for a particular service. Therefore, it cannot block

only incoming or outgoing connection attempts; it must block all communications associated with the service.

Additional differences with UDP relate to logging and notification. With TCP, even if no service is active on a particular port, Norton Personal Firewall is notified of access attempts to that port and can log those access attempts. In general, Norton Personal Firewall is not notified of access attempts to UDP ports that are not active. It does not log or notify on these attempts, and the attempts are not included in the Access History log.

If you enable UDP protection, it logs the UDP access attempts even if the UDP ports are not active.

See "Change logging preferences" on page 45.

Since UDP is connectionless, Norton Personal Firewall logs and notifies on every UDP *packet* for active ports that it is protecting (if the appropriate options have been configured). You may not want to log allowed accesses if you have enabled UDP protection, due to the number of log entries that could be generated. For example, since *DNS* uses a UDP port, the log would contain an entry for every time that you connected to a Web site.

Troubleshooting in Norton Personal Firewall

7

Frequently asked questions

Scan this section for common firewall problems.

How do I turn off firewall protection?

Turn off firewall protection in the Setup window.

To turn off firewall protection in the Setup window

1. Open Norton Personal Firewall.
2. If the Setup window does not appear, on the Tools menu, click **Setup**.
3. In the Setup window, uncheck **Enable Norton Personal Firewall**.

To disable Norton Personal Firewall for a specified amount of time

1. On the Finder menu bar, click the Norton QuickMenu icon.
2. On the Norton QuickMenu, click **Norton Personal Firewall > Disable firewall temporarily**.
3. In the Temporarily Disable Firewall window, type the number of minutes for which you want Norton Personal Firewall to be disabled.
4. Click **Disable**.

Why can't I access any Web site?

You have probably enabled *UDP* protection and have affected a low-level *service* that your computer needs to perform Internet activities. Possibilities include:

- *DHCP*: Check the *TCP/IP* settings in the Network System Preferences dialog box to see if your computer is configured to get its *IP address* using DHCP. If it is, Norton Personal Firewall has created a service entry for DHCP. Edit that service entry to allow the DHCP server access to your computer. Use the DHCP server's IP address from the Access History log.
- *DNS*: Almost all outgoing Internet operations require DNS, which converts *host names* to IP addresses. Make sure that you are not blocking the dynamic *ports* used by DNS (usually ports 32768 or higher).
- Make sure that you have checked the option to allow essential services in your protection settings. This option prevents interference with DHCP, DNS, and other standard Internet services.

What service does this port number represent?

Following are TCP and *UDP port* numbers commonly used by Macintosh *services*.

TCP port numbers

Port	Usage	Notes
20	FTP data	Used only as a source port
21	FTP control	
23	Telnet	Common port for attacks
25	SMTP (email)	
53	DNS	Mainly uses UDP, not TCP
70	Gopher	
79	Finger	
80	HTTP (Web)	
88	Kerberos	
105	PH (directory)	
106	Poppass (change password)	
110	POP3 (email)	
111	Remote procedure call (RPC)	Used for many UNIX programs

Port	Usage	Notes
113	AUTH	
119	NNTP (news)	
139	NETBIOS session	Windows access (ASIP 6)
143	IMAP (new email)	
311	AppleShare Web Admin	ASIP 6.1 and later
384	ARNS (tunneling)	
387	AURP (tunneling)	
389	LDAP (directory)	
407	Timbuktu 5.2 or later	Previous versions use other ports
427	SLP (service location)	Only uses TCP for large responses
443	SSL (HTTPS)	
497	Retrospect	UDP for finding clients
510	FirstClass server	
515	LPR (printing)	
548	AFP (AppleShare)	
554	RTSP (QuickTime server)	Also uses UDP 6970+
591	FileMaker Pro Web	Recommended alternate to 80
626	IMAP Admin	Apple extension in ASIP 6
660	ASIP Remote Admin	ASIP 6.3 and later
666	Now contact server	Violates actual port assignment
687	ASIP shared U&G port	ASIP 6.2 and later
1080	WebSTAR Admin	WebSTAR port number plus 1000
1417	Timbuktu Control (pre-5.2)	Login is through UDP Port 407
1418	Timbuktu Observe (pre-5.2)	Login is through UDP Port 407
1419	Timbuktu Send Files (pre-5.2)	Login is through UDP Port 407
1420	Timbuktu Exchange (pre-5.2)	Login is through UDP Port 407
1443	WebSTAR/SSL Admin	WebSTAR port number plus 1000

Port	Usage	Notes
3031	Program linking (Apple events)	Mac OS 9 and later
4000	Now public event server	
4199	EIMS Admin	
4347	LANsurveyor responders	Uses UDP also
5003	FileMaker Pro	Direct access, not through Web; UDP for host list
5190	AOL Instant Messenger	
5498	Hotline tracker	UDP port 5499 for finding servers
5500	Hotline server	
5501	Hotline server	
7070	RealPlayer	Also UDP ports 6970–7170
7648	CuSeeMe (video)	Client connections; UDP for audio/video
7649	CuSeeMe (video)	Connection establishment
8080	Common HTTP alternate	
19813	4D server	Previously 14566 (6.0 and earlier)

UDP port numbers

Port	Usage	Notes
53	DNS	Sometimes uses TCP
68	Dynamic Host Configuration Protocol (DHCP)	Commonly used to obtain a computer's IP address
69	Trivial File Transfer Protocol (TFTP)	
123	Network Time Protocol	
137	Windows Name Service	
138	Windows Datagram Service	
161	Simple Network Management Protocol (SNMP)	

Port	Usage	Notes
407	Timbuktu	Handshaking only, prior to version 5.2
458	QuickTime TV	
497	Retrospect	Finding clients on the network
514	Syslog	
554	Real Time Streaming Protocol (QuickTime)	
2049	Network File System (NFS)	
3283	Apple Network Assistant	
5003	FileMaker Pro	For obtaining host list
6970 +	QuickTime and RealPlayer	
7070	RTSP alternate (RealPlayer)	

How do I create a new log file?

If your log file is becoming unwieldy due to its size, you may want to start over with a new log file. You do not have to delete the old log file, and can save it for record keeping.

If you do not disable logging before renaming or moving the log file, Norton Personal Firewall continues logging to that file until logging is disabled or the computer is restarted, after which the new file is created.

To create a new log file

1. Open Norton Personal Firewall.
2. On the Personal Firewall menu, click **Preferences**.
3. In the Personal Firewall Preferences window, click **Logging**.
4. Disable logging.

See "Disable logging" on page 45.

5 Do one of the following:

- Rename the log file (called Norton Personal Firewall Log).
- Move the log file out of Library:Application Support:Norton Solutions Support:Norton Personal Firewall folder.

6 Enable logging.

See "Change logging preferences" on page 45.

Why doesn't Norton Personal Firewall load?

It may have crashed. Try deleting the preferences file, named com.symantec.NPF.plist, in Library:Preferences.

Why doesn't File Sharing work?

See "Set protection for standard Internet services" on page 51.

You may have enabled File Sharing over *TCP/IP*. By default, all TCP/IP *services* are initially protected from any access. You must specify access to File Sharing before it will be accessible.

Why can't I install Norton Personal Firewall for Mac OS X?

You must have an Administrator password to install Norton Personal Firewall in Mac OS X.

Why can't I create an alias to Norton Personal Firewall?

If Norton Personal Firewall was installed under a different Mac OS X login than the one you are currently using, you cannot create an *alias* to it because of the access permissions established in Mac OS X. Have the person who installed the software create an alias and place the alias in an area to which you have access. You can then drag the alias to the desired location.

My entries in IPFW keep disappearing

Norton Personal Firewall writes to IPFW with its own settings. Any entries that you make independently in IPFW are overwritten.

Questions about home networking

Scan this section if you have a home network.

How do I protect all of the computers on my home network?

Install a copy of Norton Personal Firewall only on those computers with access to the Internet. If other computers are networked, but do not have Internet access, they do not need Norton Personal Firewall.

All computers connected to an AirPort should have a copy of Norton Personal Firewall installed.

How do I specify access for a computer with a dynamically generated IP address?

See "To view the Access History log" on page 41.

Computers that get their *IP addresses* from *DHCP* (Dynamic Host Configuration *Protocol*) usually don't have the same IP address every time they connect to a network. However, their IP addresses usually fall within a given range. Determine that range by checking the Access History log for denied accesses to that computer and noting the IP addresses used.

See "To add a range of addresses" on page 53.

You can then specify that range in the IP address list for the *service* for which you need to define access.

How does the firewall affect file and printer sharing?

See "Set protection for standard Internet services" on page 51.

Norton Personal Firewall provides security for *TCP/IP* connections. It does not affect *AppleTalk* connections in Mac OS 8.1 to 9.x. If you require that other computers have access to File Sharing on your computer through TCP/IP, include their *IP addresses* in the allow access list for File Sharing.

In Mac OS X, AppleTalk also uses TCP/IP for File Sharing and program linking. Make sure that File Sharing and program linking access is allowed for those computers to which you connect using AppleTalk.

Keeping Norton Personal Firewall up-to-date

8

When you first install your Symantec product and run LiveUpdate, you have the most current versions of the product and any protection-related files, such as the inappropriate Web site list for Norton Internet Security or the *virus definitions* list for Norton AntiVirus.

At any time, new *threats* can be introduced. Also, some operating system updates may necessitate changes to a program. When these events occur, Symantec provides new files to address these issues. You can get these new files by using LiveUpdate.

Using your existing Internet connection, LiveUpdate connects to the Symantec LiveUpdate server, checks for available updates, then *downloads* and installs them.

About program updates

Program updates are minor improvements to your installed product, usually available for *download* from a Web site. These differ from product upgrades, which are newer versions of entire products. Program updates that replace sections of existing software are called patches. Patches are usually created to ensure the compatibility of a program with new versions of operating systems or hardware, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of downloading and installing program updates. It locates and downloads files from an Internet site, then installs them, and deletes the leftover files from your computer.

When you should update

See "Schedule future updates" on page 74.

During installation of your software, you have the option to run LiveUpdate. You should do so to ensure that you have the most up-to-date protection files. After installation, if you have Norton AntiVirus, Norton Personal Firewall, Norton Internet Security, or Norton SystemWorks installed, update at least once a month to ensure that you have the latest *virus definitions* and firewall protection.

Before updating

In some cases there are preparations you must make before running LiveUpdate. For example, if you use America Online (AOL) as your *Internet service provider* (ISP), you must log on to AOL before you use LiveUpdate.

If you use America Online to connect

If you use America Online (AOL) as your *Internet service provider* (ISP), you need to log on to AOL before you use LiveUpdate.

To use LiveUpdate with AOL

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Open LiveUpdate.
4. Follow the instructions in "Update procedures" on page 72.
5. When the LiveUpdate session is complete, close your AOL browser. If your LiveUpdate session requires that you restart your computer, disconnect from AOL before restarting.

If you update on an internal network

If you run LiveUpdate on a Macintosh that is connected to a network that is within a company firewall, your network administrator might set up an internal LiveUpdate server on your network. Once your administrator has configured it, LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

If you can't use LiveUpdate

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new update files from the Symantec Web site.

Your subscription must be current to obtain new protection updates from the Symantec Web site.

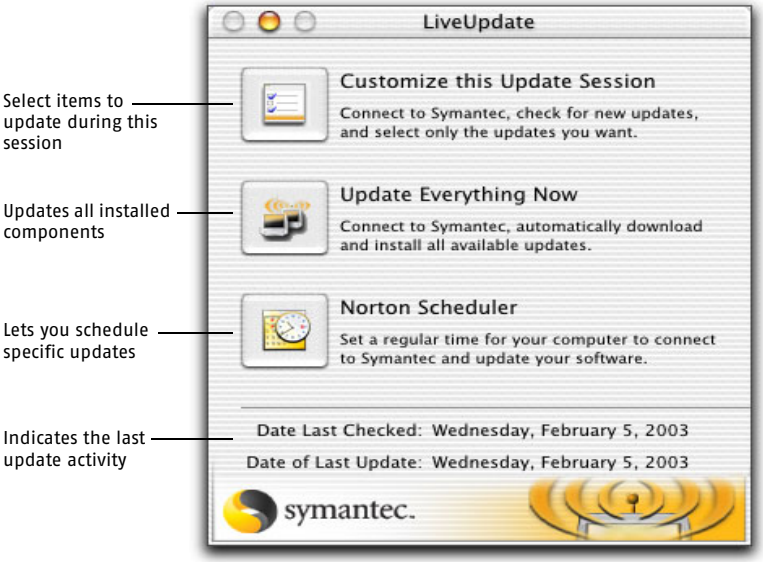
To obtain product updates from the Symantec Web site

1. Open your Internet browser and go to the following site: securityresponse.symantec.com/downloads/
2. On the downloads page, in the product updates list, select the product for which you want an update.
3. On the support page, select the version of the product.
4. Click **continue**.
5. On the product page, select the file to download.
   Information about the update is included with the download.

Update procedures

See "Schedule future updates" on page 74.

You can have LiveUpdate look for all updates at once, or select individual items to update. You can also schedule a future LiveUpdate session.


Select items to update during this session
Updates all installed components
Lets you schedule specific updates
Indicates the last update activity
LiveUpdate
Customize this Update Session
Connect to Symantec, check for new updates, and select only the updates you want.
Update Everything Now
Connect to Symantec, automatically download and install all available updates.
Norton Scheduler
Set a regular time for your computer to connect to Symantec and update your software.
Date Last Checked: Wednesday, February 5, 2003
Date of Last Update: Wednesday, February 5, 2003
symantec.

Update everything now

Updating all available files is the fastest method to ensure the latest protection for all your Symantec products.

To update everything now

1. Click and hold down the mouse button on the Norton Personal Firewall icon in the Dock to open the Dock menu.
2. On the Dock menu, click **LiveUpdate**.
3. Click **Update Everything Now**.
   A status dialog box keeps you informed of the file transfer process.

Customize a LiveUpdate session

If you want to update only one or two items, you can select them and omit items that you don't want to update.

To customize a LiveUpdate session

1 In the LiveUpdate window, click **Customize this Update Session**. LiveUpdate presents a list of available updates. By default, all are checked for inclusion in this update session. If your files are already up-to-date, no items are available for selection.

2 Uncheck the items that you don't want to update.

3 Click **Update**.
The file transfer takes a few minutes. When it is complete, the LiveUpdate summary window appears.

See "View the LiveUpdate Summary" on page 73.

After updating

When a LiveUpdate session is complete, the LiveUpdate Summary window displays a list of what was updated, along with brief notes.

View the LiveUpdate Summary

The LiveUpdate Summary dialog box displays a summary of the activity and a list of products updated in this session.

Some updates require that you restart your computer. When this recommendation appears in the summary description, the Restart button is available.

To restart after a LiveUpdate session

❖ In the LiveUpdate Summary window, click **Restart**.

Empty the Trash after a LiveUpdate session

After you update program files, LiveUpdate moves the older, discarded files to the Trash. If you haven't already restarted after updating, you might get a message that these files are in use. After you restart your computer, you can empty the Trash.

Check product version numbers and dates

The LiveUpdate window displays the version numbers and dates of the most recent updates.

You can also check the version numbers and dates in the product's About box, accessible from the product menu, to verify that you have the latest version.

To view an application's About box

1. Open your product.
2. On the product menu, click **About <product name>**.
   The About box lists the version number and copyright dates.
3. When you've finished viewing the About box, close it.

Schedule future updates

The user who scheduled the event must be logged on for the scheduled event to occur. If this condition is not true, the event occurs the next time the correct user is logged on.

You can set up events to run at a scheduled time, without your participation. If your Macintosh is turned off during the time an event should take place, the event occurs the next time that you start your Macintosh. Before scheduling an update, test it once manually. See "Update everything now" on page 72, and "Customize a LiveUpdate session" on page 72.

For instructions on scheduling future updates, see "Schedule LiveUpdate events" on page 76.

Scheduling future events

9

Use Norton Scheduler to ensure that key tasks are performed regularly to keep your computer and data protected.

About Norton Scheduler

The tasks that are available in Norton Scheduler depend on what products are installed.

If your Macintosh is turned off during the time that an event should take place, the event occurs the next time that you start your Macintosh.

Open Norton Scheduler

You can open Norton Scheduler from your open program.

To open Norton Scheduler from Norton Personal Firewall

1. Open Norton Personal Firewall.
2. Click and hold down the mouse button on the Norton Personal Firewall icon in the Dock to open the Dock menu.
3. On the Dock menu, click **Norton Scheduler**.

To open Norton Scheduler from LiveUpdate

See "Update procedures" on page 72.

1. Open LiveUpdate.
2. In the LiveUpdate window, click **Norton Scheduler**.

Schedule LiveUpdate events

In Norton Scheduler, LiveUpdate events check for updates to your installed products. If you have Norton AntiVirus installed, a monthly *virus definitions* update is also scheduled.

To add scheduled LiveUpdate events

See "Open Norton Scheduler" on page 75.

1. Open Norton Scheduler.
2. In the Norton Scheduler window, click **New**.
3. Click **Product Update**.
4. Type a descriptive name for the LiveUpdate task, for example, Update Fridays.
5. In the Choose a product to update list, select the item to update. Your options are:

All Products	Updates all installed products.
Virus Definitions	Updates virus definitions.
LiveUpdate	Updates LiveUpdate program files.
<Product Name>	Updates a product that you select. The names of installed Symantec products appear in the list.

6. In the Set a Frequency list, specify when the update should occur. Your options are:

Monthly	Runs the event monthly on the indicated date and time. You can select a date from the first of the month to the twenty-eighth.
Weekly	Updates once a week on the specified day and at the specified time.
Daily	Runs the event daily at the indicated time.
Annually	Runs the event each year on the indicated day and time. You can schedule the event up to one year in advance.

7. If you choose a frequency other than Daily, specify the date or day of the week that the update should occur.

See "Set a start time" on page 77.

8 Set a start time for the event.

9 Click **Save**.

Set a start time

You can set the exact time at which you want a scheduled event to start.

To set a start time

1 In the task window, in the Set the time box, do one of the following:

- Type the exact time that you want in the hour and minute boxes.
- Select the hour or minute box, then click the Up Arrow or Down Arrow to change the time that is displayed.

2 If your computer is set to display a 12-hour clock, an AM/PM indicator appears next to the time. Click the indicator to toggle the setting.

3 When you are finished, click **Save**.

Manage scheduled events

You can edit, delete, disable, and reset scheduled events.

Edit scheduled events

You can make changes to the events that you schedule.

To edit a scheduled event

1 Open Norton Scheduler.

2 In the Scheduled Events list, select the scheduled event that you want to change.

3 Click **Edit**.

4 Make your changes.
For a description of the scheduling options, see "Schedule LiveUpdate events" on page 76.

5 To change the event name, type a new name in the name field.

6 Click **Save**.

Delete scheduled events

You can delete scheduled events that you no longer want.

To delete a scheduled event

1. Open Norton Scheduler.
2. In the Scheduled Events list, select the scheduled event that you want to delete.
3. Click **Delete**.
4. In the verification box that appears, click **Delete** to verify that you want to delete the event.

Disable scheduled events

You can disable scheduled events without deleting them in case you want to enable them later.

To disable a scheduled event

1. In the Scheduled Events list, under On, uncheck the event that you want to disable.
2. To enable the event, check it again.

Reset scheduled tasks

You can reset all scheduled tasks to their original installed settings.

Product	Installed settings
Norton Personal Firewall	None.
Norton AntiVirus	Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month.
Norton Internet Security	Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month.
Norton Utilities	Daily FileSaver snapshot to update your disk directory information. Set to run at noon. Daily Speed Disk defragmentation. Set to run at midnight.
Norton SystemWorks	Monthly LiveUpdate task to check for new virus definitions. Set to run on the first of each month. Daily Speed Disk defragmentation. Set to run at midnight. Daily FileSaver snapshot to update your disk directory information. Set to run at noon.

To reset scheduled tasks

1. On the Norton Scheduler menu, click **Reset Scheduled Tasks**.
2. In the verification window, click **Reset**.

Service and support solutions

The Service & Support Web site at http://service.symantec.com supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at http://service.symantec.com tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:
http://www.symantecstore.com

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- Online Service and Support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.

- PriorityCare telephone support

  This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at:
http://service.symantec.com

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Authorized Service Center
Postbus 1029
3600 BA Maarssen,
The Netherlands

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Latin America

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12 andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

Portuguese:
http://www.service.symantec.com/br
Spanish:
http://www.service.symantec.com/mx
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

April 2, 2003

Glossary

access privileges	The types of operations that a user can perform on a system resource. For example, a user can have the ability to access a certain directory and open, modify, or delete its contents.
ActiveSync	The synchronization software for Microsoft Windows-based Pocket PCs.
ActiveX	A method of embedding interactive programs into Web pages. The programs, which are called controls, run when you view the page.
alert	A message that appears to signal that an error has occurred or that there is a task that requires immediate attention, such as a system crash or a Virus Alert.
alias	A shortcut icon that points to an original object such as a file, folder, or disk.
AppleTalk	A protocol that is used by some network devices such as printers and servers to communicate.
attack signature	A data pattern that is characteristic of an Internet attack. Intrusion Detection uses attack signatures to distinguish attacks from legitimate traffic.
beam	To transfer certain programs and data between two handheld devices using built-in infrared technology.

boot record	A sector at the start of a disk that describes the disk (sector size, cluster size, and so on). On startup disks, the boot record also has a program that loads the operating system.
bootable disk	A disk that can be used to start a computer.
cache	A location on your disk in which data is stored for reuse. A Web browser cache stores Web pages and files (such as graphics) as you view them.
cache file	A file that is used to improve the performance of Windows.
compressed file	A file whose content has been made smaller so that the resulting data occupies less physical space on the disk.
connection-based protocol	A protocol that requires a connection before information packets are transmitted.
connectionless protocol	A protocol that sends a transmission to a destination address on a network without establishing a connection.
cookie	A file that some Web servers put on your disk when you view pages from those servers. Cookies store preferences, create online shopping carts, and identify repeat visitors.
denial-of-service attack	A user or program that takes up all of the system resources by launching a multitude of requests, leaving no resources, and thereby denying service to other users.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that assigns a temporary IP address to each device on a network. DSL and cable routers use DHCP to allow multiple computers to share a single Internet connection.
dial-up	A connection in which a computer calls a server and operates as a local workstation on the network.
DNS (Domain Name System)	The naming system used on the Internet. DNS translates domain names (such as www.symantec.com) into IP addresses that computers understand (such as 206.204.212.71).

DNS server (Domain Name System server)	A computer that maps domain names to IP addresses. When you visit www.symantec.com, your computer contacts a DNS server that translates the domain name into an IP address (206.204.212.71).
domain	The common Internet address for a single company or organization (such as symantec.com). See also host name.
DOS window	A method of accessing the MS-DOS operating system to execute DOS programs through the Windows graphical environment.
download	To transfer a copy of a file or program from the Internet, a server, or computer system to another server or computer.
driver	Software instructions for interpreting commands for transfer to and from peripheral devices and a computer.
encryption	Encoding data in such a way that only a person with the correct password or cryptographic key can read it. This prevents unauthorized users from viewing or tampering with the data.
Ethernet	A common method of networking computers in a LAN (local area network). Ethernet cables, which look like oversized phone cables, carry data at 10M bps or 100M bps.
executable file	A file containing program code that can be run. Generally includes any file that is a program, extension, or system files whose names end with .bat, .exe, or .com.
extension	The three-letter ending on a file name that associates the file with an activity or program. Examples include .txt (text) and .exe (executable program).
FAT (file allocation table)	A system table (used primarily by DOS and Windows 9x/Me) that organizes the exact location of the all files on the hard drive.
file type	A code that associates the file with a program or activity, often appearing as the file name extension, such as .txt or .jpeg.

Finder	The program that manages your Macintosh disk and file activity and display.
firewall rule	Parameters that define how a firewall reacts to specific data or network communications. A firewall rule usually contains a data pattern and an action to take if the pattern is found.
fragmented	When the data that makes up a file is stored in noncontiguous clusters across a disk. A fragmented file takes longer to read from the disk than an unfragmented file.
fragmented IP packet	An IP packet that has been split into parts. Packets are fragmented if they exceed a network's maximum packet size, but malicious users also fragment them to hide Internet attacks.
FTP (File Transfer Protocol)	An application protocol used for transferring files between computers over TCP/IP networks such as the Internet.
hidden attribute	A file attribute that makes files harder to access and more difficult to delete than other files. It also prevents them from appearing in a DOS or Windows directory list.
host name	The name by which most users refer to a Web site. For example, www.symantec.com is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS.
HotSync	The synchronization software for Palm OS handheld devices.
HTML (Hypertext Markup Language)	The language used to create Web pages.
ICMP (Internet Control Message Protocol)	An extension to the basic Internet Protocol (IP) that provides feedback about network problems.
IGMP (Internet Group Management Protocol)	An extension to the basic Internet Protocol (IP) that is used to broadcast multimedia over the Internet.

IMAP4 (Internet Message Access Protocol version 4)	One of the two most popular protocols for receiving email. IMAP makes messages available to read and manage without downloading them to your computer.
infrared (IR) port	A communication port on a handheld device for interfacing with an infrared-capable device. Infrared ports do not use cables.
IP (Internet Protocol)	The protocol that underlies most Internet traffic. IP determines how data flows from one computer to another. Computers on the Internet have IP addresses that uniquely identify them.
IP address (Internet Protocol address)	A numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually shown as four groups of numbers separated by periods. For example, 206.204.52.71.
ISP (Internet service provider)	A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.
Java	A programming language used to create small programs called applets. Java applets can be used to create interactive content on Web pages.
JavaScript	A scripting language used to enhance Web pages. Most sites use JavaScript to add simple interactivity to pages, but some use it to open pop-up ads and reset visitors' homepages.
macro	A simple software program that can be started by a specific keystroke or a series of keystrokes. Macros can be used to automate repetitive tasks.
NAT (network address translation)	A method of mapping private IP addresses to a single public IP address. NAT allows multiple computers to share a single public IP address. Most DSL and cable routers support NAT.
network address	The portion of an IP address that is shared by all computers on a network or subnet. For example, 10.0.1.1 and 10.0.1.8 are part of the network address 10.0.1.0.

NTFS (NTFS file system)	A system table (used primarily by Windows 2000/ XP) that organizes the exact location of all the files on the hard drive.
packet	The basic unit of data on the Internet. Along with the data, each packet includes a header that describes the packet's destination and how the data should be processed.
partition	A portion of a disk that is prepared and set aside by a special disk utility to function as a separate disk.
POP3 (Post Office Protocol version 3)	One of the two most popular protocols for receiving email. POP3 requires that you download messages to read them.
port	A connection between two computers. TCP/IP and UDP use ports to indicate the type of server program that should handle a connection. Each port is identified by a number.
port number	A number used to identify a particular Internet service. Internet packets include the port number to help recipient computers decide which program should handle the data.
PPP (Point-to-Point Protocol)	A protocol for communication between two computers using a dial-up connection. PPP provides error-checking features.
protocol	A set of rules governing the communication and transfer of data between computers. Examples of protocols include HTTP and FTP.
proxy	A computer or program that redirects incoming and outgoing traffic between computers or networks. Proxies are often used to protect computers and networks from outside threats.
registry	A category of data stored in the Windows registry that describes user preferences, hardware settings, and other configuration information. Registry data is accessed using registry keys.
removable media	Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, CDs, DVDs, and Zip disks.

router	A device that forwards information between computers and networks. Routers are used to manage the paths that data takes over a network. Many cable and DSL modems include routers.
script	A program, written in a scripting language such as VBScript or JavaScript, that consists of a set of instructions that can run without user interaction.
service	General term for the process of offering information access to other computers. Common services include Web service and FTP service. Computers offering services are called servers.
SSL (Secure Sockets Layer)	A protocol for secure online communication. Messages sent using SSL are encrypted to prevent unauthorized viewing. SSL is often used to protect financial information.
subnet	A local area network that is part of a larger intranet or the Internet.
subnet mask	A code, in the form of an IP address, that computers use to determine which part of an IP address identifies the subnet and which part identifies an individual computer on that subnet.
synchronize	The process by which a handheld device and computer compare files to ensure that they contain the same data.
sync	The process of transferring programs and data from a computer to a handheld device.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	Standard protocols used for most Internet communication. TCP establishes connections between computers and verifies that data is properly received. IP determines how the data is routed.
threat	A program with the potential to cause damage to a computer by destruction, disclosure, modification of data, or denial of service.
Trojan horse	A program containing malicious code that is disguised as or hiding in something benign, such as a game or utility.

UDP (User Datagram Protocol)	A protocol commonly used for streaming media. Unlike TCP, UDP does not establish a connection before sending data and it does not verify that the data is properly received.
virus definition	Virus information that an antivirus program uses to identify and alert you to the presence of a specific virus.
wildcard characters	Special characters (like *, $, and ?) that act as placeholders for one or more characters. Wildcards let you match several items with a single specification.
worm	A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down. So far, worms do not exist in the Macintosh world.

Index

A

access
  allowing and denying 10
  determining with Norton Personal Firewall 11
  monitoring 35
  responding to attempts 40
  restricting 24
  tracking attempt, with Norton Personal Firewall 33
  types 41
Access History
  customizing 42
  exporting data 42
  log 40
  reviewing in Norton Personal Firewall 41
  window 11
active FTP support 10, 57
addresses, IP 32
alerts in Norton Personal Firewall 40
America Online
  connecting before LiveUpdate 70
  connecting to Symantec Web site 20
  registering your product 20
AppleTalk
  and Norton Personal Firewall 33
  in Mac OS X 33
  vs. TCP/IP, security issues 33
application. *See* program
automatic setup
  described 9
  notifications 36

B

blocking outgoing connections, example 10
Bluetooth 31

C

computers
  host names 32
  intrusion protection 9, 31
  IP addresses 32
Connected Users report 47
connections
  blocking with Norton Personal Firewall 10
  TCP/IP 31
  UDP 31
custom services
  changing or deleting 55
  defining 54
customizing
  LiveUpdate 72
  Norton Personal Firewall 51
  services 55
  toolbars 27

D

deleting
  custom services 55
  IP addresses 56
denial-of-service attacks 57
disabling protection 26
disconnected users time limit 50
disconnecting a user 49
DNS 32
domain name addresses 32
domain names, Internet 32

E

enabling protection 26
essential services 10, 59

F

features in Mac OS X 9
firewalls
  about 10
  customizing 51
  enabling and disabling protection 26
  monitoring activity 35
  troubleshooting 61
  what they do 10
frequently asked questions (FAQ) 61

G

glossary terms 29

H

hacker attacks 9
Help 28
host names, Internet 32

I

ICMP 57
ignore access attempts 57
Inspector window 43
installing on Mac OS X 10.1.5 15
Internet
  connections, blocking with Norton Personal Firewall 10
  domain names 32
  firewalls 10
  host names 32
  intrusion detection 10
  intrusion protection 9, 31
  IP addresses 32
  protection with port numbers 32
  setting protection 24
  types of access attempts 41
  using to register your product 19
Internet links, late breaking news 20
intrusions
  protecting from 9, 31
  responding to attempts 35
IP addresses 32
  changing list 56
  finding with Norton Personal Firewall 32
  restricting or allowing access 24, 52
  spoofed 58
IPFW 66

K

keeping files current 69
Knowledge Base 30

L

Late Breaking News, reading 20
Learn More Web site 44, 49
LiveUpdate
  checking file dates 73
  customizing 72
  emptying Trash 73
  keeping current with 69
  running during installation 18
  scheduled events 76
  updating files 72
  using with America Online 70
  viewing summary 73
log file
  creating new 65
  format 46

log file *(continued)*
location 46
log structure, for Norton Personal Firewall 46
logging, preferences in Norton Personal Firewall 45

M

Macintosh network protocols 33

N

new features 9
News, Late Breaking 20
Norton Personal Firewall 55
access responses 40
access types 41
alert messages 40
and AppleTalk 33
custom services 55
customizing 51
customizing protection 54
default settings 11
determining access 11
enabling and disabling protection 26
enabling or disabling notification 36
finding IP addresses 32
Learn More Web site 44, 49
log structure 46
logging preferences 45
monitoring activity 35
Quick Check 35
reviewing access history 41
Self Test 35
Setup window 24
tracking access attempts 33
troubleshooting 61
uninstalling 21
Visual Tracking Web site 44, 49
what is protected 10, 31
Norton QuickMenu 10
to disable firewall protection 27
to open Norton Personal Firewall 23
Norton Scheduler
changing events 77
Norton Scheduler *(continued)*
deleting events 77
described 75
resetting events 78
notifications 36

O

outgoing connection protection 10

P

PDF 28, 29
Ping requests 57
port numbers, creating protection 32
preferences
access notification 36
disconnected users time limit 50
file location 66
logging, in Norton Personal Firewall 45
program
registering 19
registering using America Online 20
starting 23
program files, updating with LiveUpdate 72
protection
provided by Norton Personal Firewall 10, 31
with port numbers 32

Q

Quick Check 37

R

Read Me file 14, 29
registering your product 19
Rendezvous networking traffic 57
reports
Access History 41
Connected Users 47
responding to access attempts 35
restarting, after installation 18
restricting access to IP address 52

S

scheduled events
  changing 77
  deleting 77
  LiveUpdate 76
  resetting 78
Security Check 39
Self Test 37
Service and Support 81
service and support Web site 30
services
  adding 54
  setting individual preferences for 36, 45, 54
settings
  access notification 36
  in Norton Personal Firewall 11
  LiveUpdate 72
  See also preferences
Setup Assistant 9, 24
Setup window, in Norton Personal Firewall 24
spoofed IP addresses 58
Stealth 57
subnets 32
Summary report 25
suspicious activity protection 10, 58
Symantec Security Check 39
Symantec Web site 30
  connecting with America Online 20
  downloading product updates 71
  Late Breaking News 20
  registration 19
  tips for searching 30
system requirements, in Read Me file 14

T

TCP/IP
  connections 31
  vs. AppleTalk, security issues 33
Technical Support 81
testing Norton Personal Firewall 35
toolbars, customizing 27
Trash, empty after LiveUpdate session 73
Trojan horses 9
troubleshooting, in Norton Personal Firewall 61

U

UDP
  address protection 32
  connections 31
  enabling protection 59
uninstalling 21
updating
  all files 72
  from Symantec Web site 71
Upgrade button during installation 17
User's Guide
  described 28
  PDF 29

V

version numbers
  viewing for products 73
  viewing with LiveUpdate 73
viewing
  access attempts 43
  latest program update 73
  versions and dates 73
viruses 9
Visual Tracking Web site 44, 49

W

Web site, Symantec 30, 71

Norton™ Personal Firewall for Macintosh®

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE. You must be a registered customer in order to receive CD replacements.

If your Symantec product was installed on your computer when you purchased it, contact your hardware manufacturer for CD replacement information.

FOR CD REPLACEMENT

Please send me: _____ CD Replacement

Name _____

Company Name _____

Street Address (No P.O. Boxes, Please) _____

City _____ State _____ Zip/Postal Code _____

Country* _____ Daytime Phone _____

Software Purchase Date _____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: _____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	_____
Shipping & Handling	$ 9.95
TOTAL DUE	_____

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%).
Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (Check One):

___ Check (Payable to Symantec) Amount Enclosed $ _____ _____Visa ____ Mastercard ____ AMEX

Credit Card Number _____Expires _____

Name on Card (please print) _____ Signature _____

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.

Symantec and Norton are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 2003 Symantec Corporation. All rights reserved. Printed in the U.S.A.

symantec™